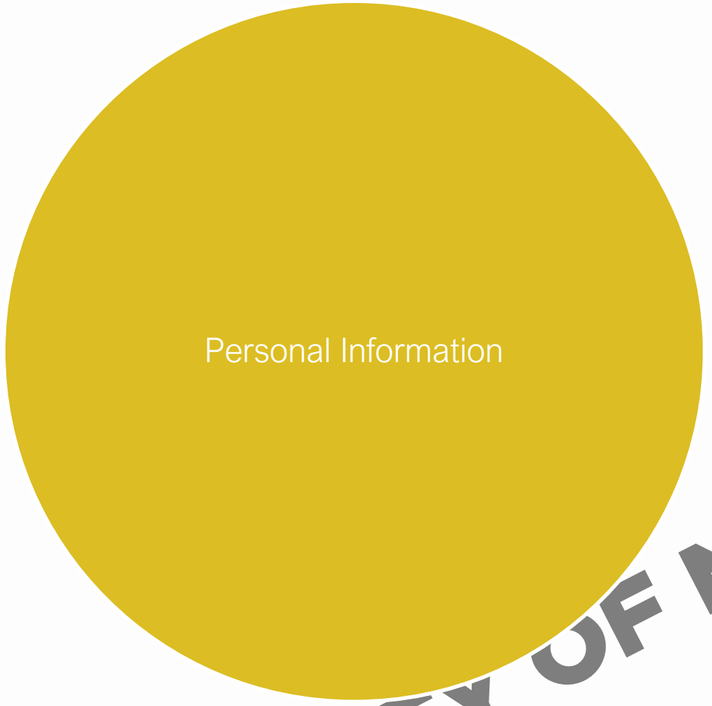
SOME

Key Concepts

Hint: It's not all about I.T.

NATIONAL
PRIVACY
COMMISSION

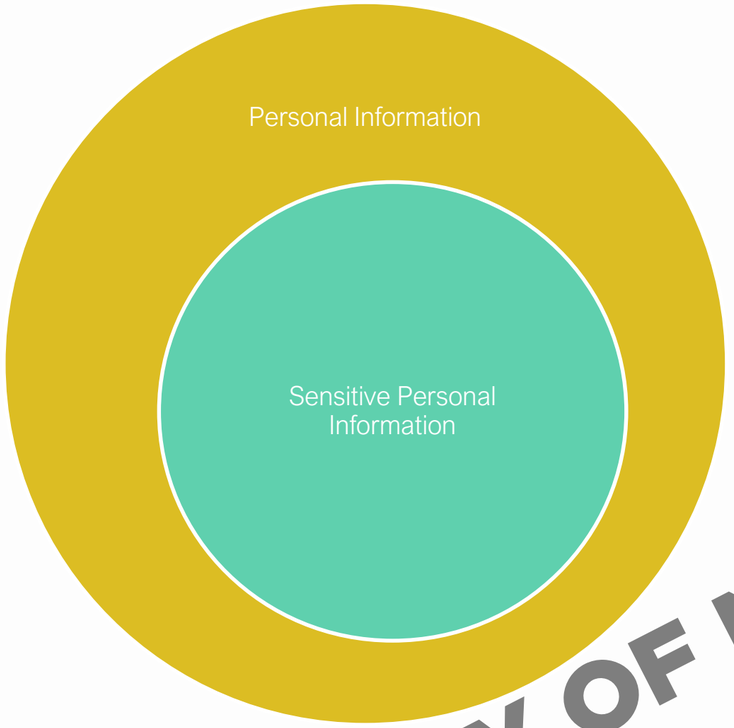
Key concepts



Personal information refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

– *RA. 10173, Section 3.g*

Key concepts



Sensitive personal information refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

– RA. 10173, Section 3.l

Personal Information	Sensitive Personal Information (List based on IRR)	Privileged Information (List based on Rules of Court)
Name	Race	Data received within the context of a protected relationship – husband and wife
Address	Ethnic origin	
Place of work	Marital status	
Telephone number	Age	
Gender	Color	Data received within the context of a protected relationship – attorney and client
Location of an individual at a particular time	Religious affiliation	
IP address	Philosophical affiliation	
Birth date	Political affiliation	
Birth place	Health	Data received within the context of a protected relationship – priest and penitent
Country of citizenship	Education	
Citizenship status	Genetics	
Payroll & benefits information	Sexual life	
Contact information	Proceeding for any offense committed or alleged to have been committed, the disposal of such proceedings, the sentence of any court in such proceedings	Data received within the context of a protected relationship – doctor and patient

	Sensitive Personal Information (List based on IRR)	
	Social security number	
	Licenses or its denials, suspension or revocation	
	Tax returns	
	Other personal info issued by government agencies	
	Bank and credit/debit card numbers	
	Websites visited	
	Materials downloaded	
	Any other information reflecting preferences and behaviors of an individual	
	Grievance information	
	Discipline information	
	Leave of absence reason	
	Licenses or its denials, suspension or revocation	

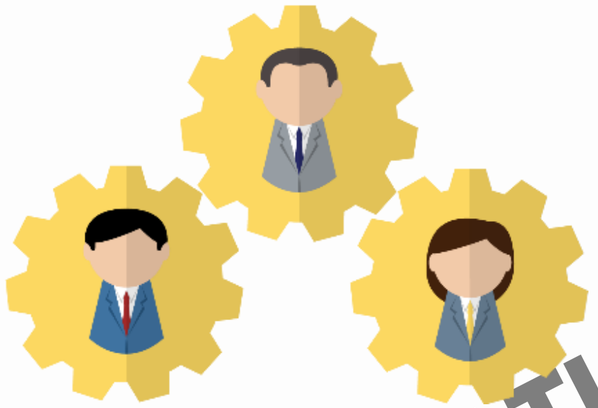
PERSONAL INFORMATION CONTROLLER

Refers to a natural or juridical person, or any other body who **controls the processing of personal data,** or instructs another to process personal data on its behalf.

It excludes:

- A natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
- A natural person who processes personal data in connection with his or her personal, family, or household affairs;

PERSONAL INFORMATION PROCESSOR



Refers to any natural or juridical person or any other body to whom a personal information controller may **outsource or instruct the processing of personal data** pertaining to a data subject.

STRUCTURE OF RA 10173

Sections 1-6.
Definitions and General Provisions

Sections 25-37.
Penalties

Sections 7-10.
The National Privacy Commission

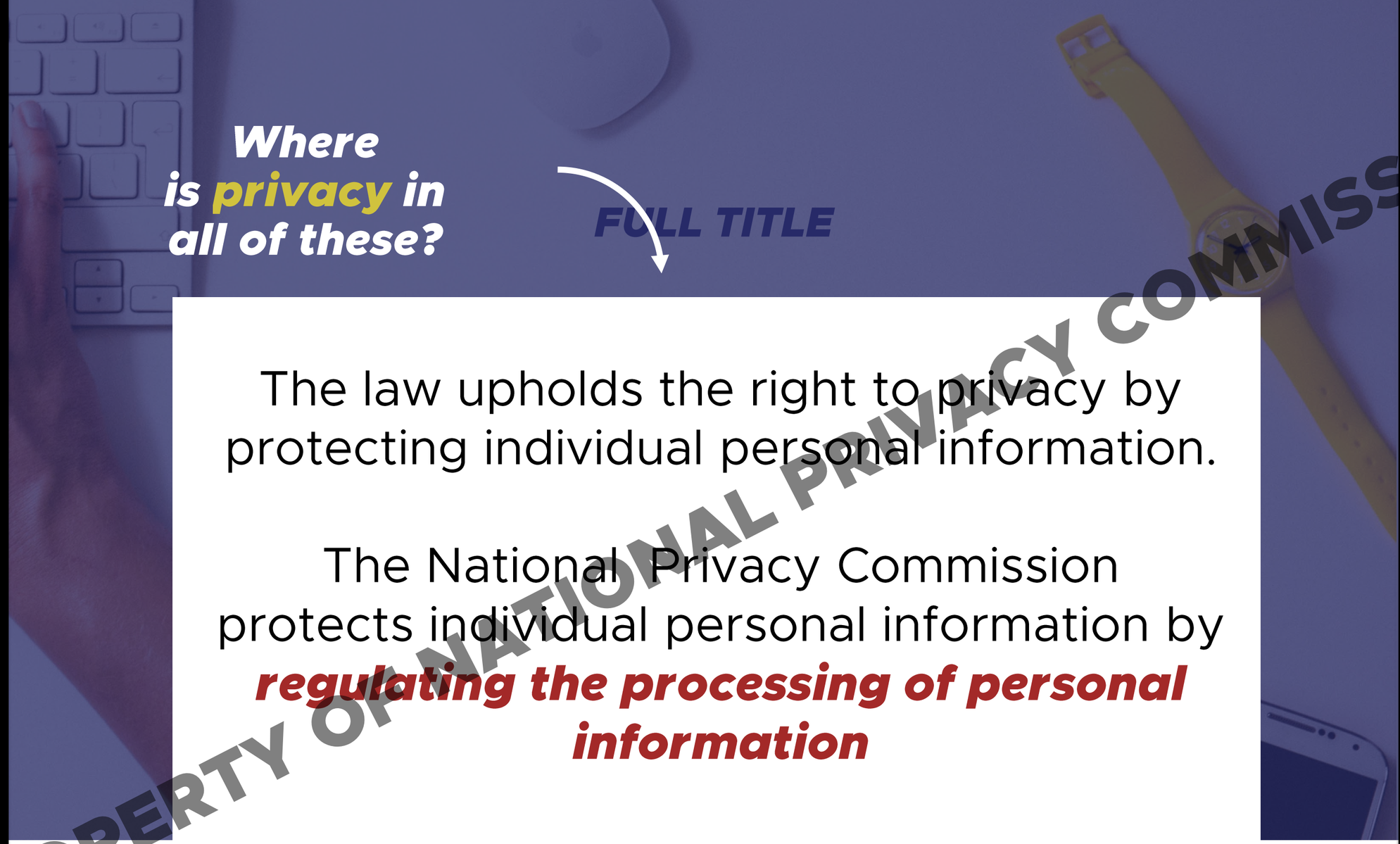
Sections 22-24.
Provisions Specific to Government

Sections 11-21.
Rights of Data Subjects, and Obligations of Personal Information Controllers and Processors

FULL TITLE

An act protecting
individual personal information in information
and communications systems in the government and
the private sector, creating for this purpose
a National Privacy Commission,
and for other purposes

NATIONAL
PRIVACY
COMMISSION



Where is privacy in all of these?

FULL TITLE

The law upholds the right to privacy by protecting individual personal information.

The National Privacy Commission protects individual personal information by ***regulating the processing of personal information***

NATIONAL PRIVACY COMMISSION

The Obligations which must be complied with by Government

Data Privacy Act of 2012

IRRs (promulgated 2016)

2016 Series (issued)

- Circular 1 — Gov't Agencies
- Circular 2 — Data Sharing
- Circular 3 — Breach Mgmt
- Circular 4 — Rules Procedure

2017 Series (planned)

- *Circular — BSP-Supervised*
- *Circular — DOH-Regulated*
- *Circular — Outsourcing Cos.*

DP 11 LOCAL GOVERNMENT UNITS

When should you comply?

NPC Circular 16-01

SECTION 36. **Transitory Period.** Government agencies shall be given a period of one (1) year transitory period from the effectivity of these Rules to comply with the requirements provided herein.

February 1, 2018

Why should you comply?

- Sec. 22. The **head of each government agency** or instrumentality shall be responsible for complying with the security requirements mentioned herein…

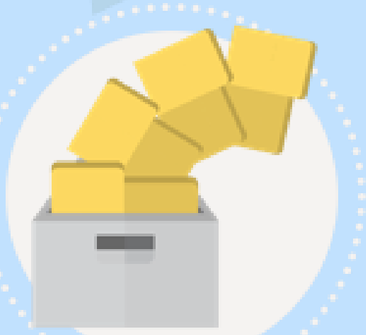
- Sec. 34. Extent of Liability. If the offender is a corporation, partnership or any juridical person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or by their gross negligence, allowed the commission of the crime.

DP 11
LOCAL GOVERNMENT UNITS

THE DATA LIFE CYCLE

CREATE AND COLLECT

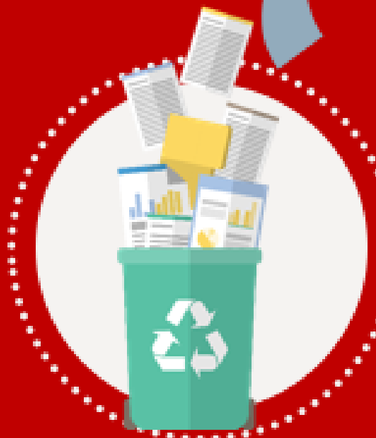
STORE AND TRANSMIT



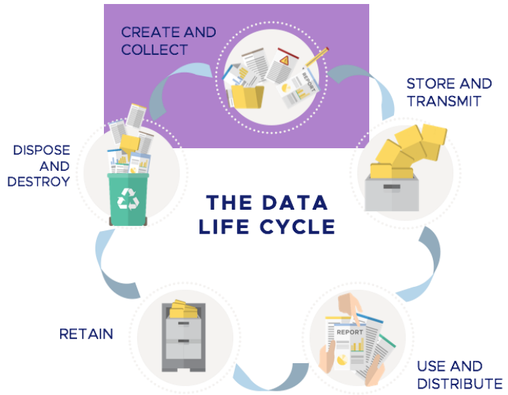
USE AND DISTRIBUTE

RETAIN

DISPOSE AND DESTROY

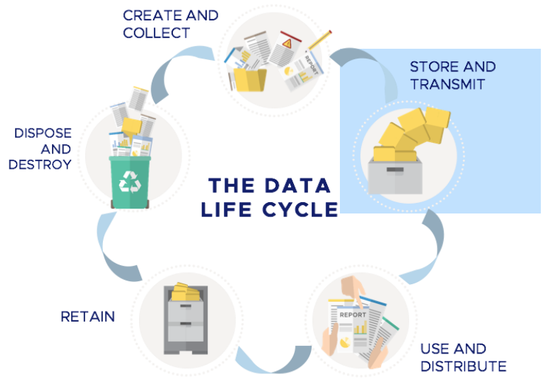


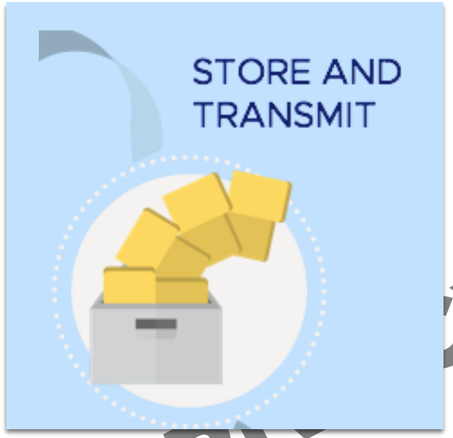
I. CREATE AND COLLECT



Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Unauthorized Processing of Personal Information/Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million

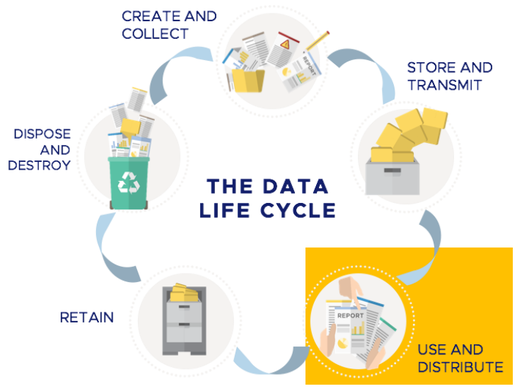
II. STORE AND TRANSMIT





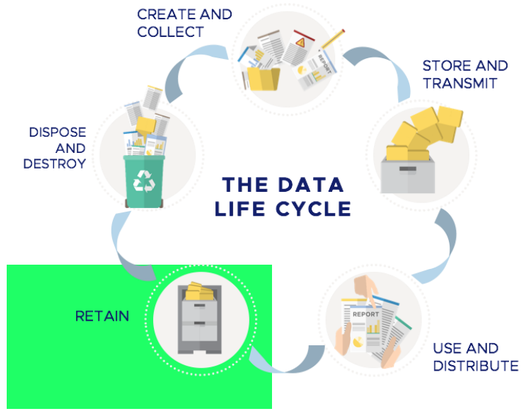
Punishable Act	Imprisonment	Fine (PHP)
Accessing of Personal Information and Sensitive Personal Information due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

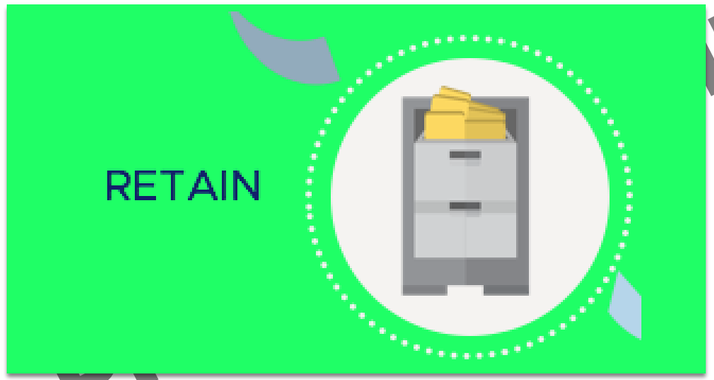
III. USE AND DISTRIBUTE



Punishable Act	Imprisonment	Fine (PHP)
Unauthorized Processing of Personal Information and Sensitive Personal Information	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Unauthorized Purposes	18 months to 5 years — 2 years to 7 years	500 thousand to 2 million
Intentional Breach	1 year to 3 years	500 thousand to 2 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 2 million

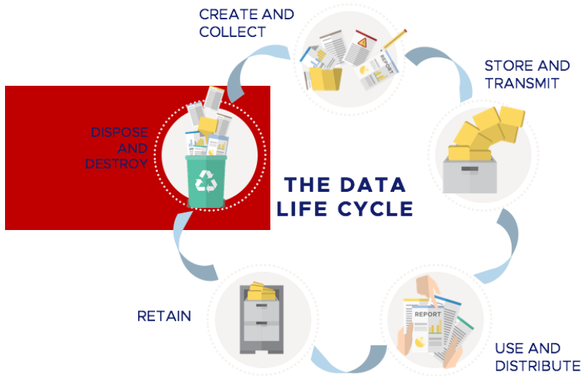
IV. RETAIN





Punishable Act	Imprisonment	Fine (PHP)
Access due to Negligence of Records	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Malicious Disclosure	18 months to 5 years	500 thousand to 1 million
Unauthorized Disclosure	1 year to 3 years — 3 years to 5 years	500 thousand to 1 million

V. DISPOSE AND DESTROY



Punishable Act	Imprisonment	Fine (PHP)
Improper Disposal of Records	6 months 2 years — 1 year to 3 years	100 thousand to 1 million
Access due to Negligence	1 year to 3 years — 3 years to 6 years	500 thousand to 4 million
Concealing Breach	18 months to 5 years	500 thousand to 1 million

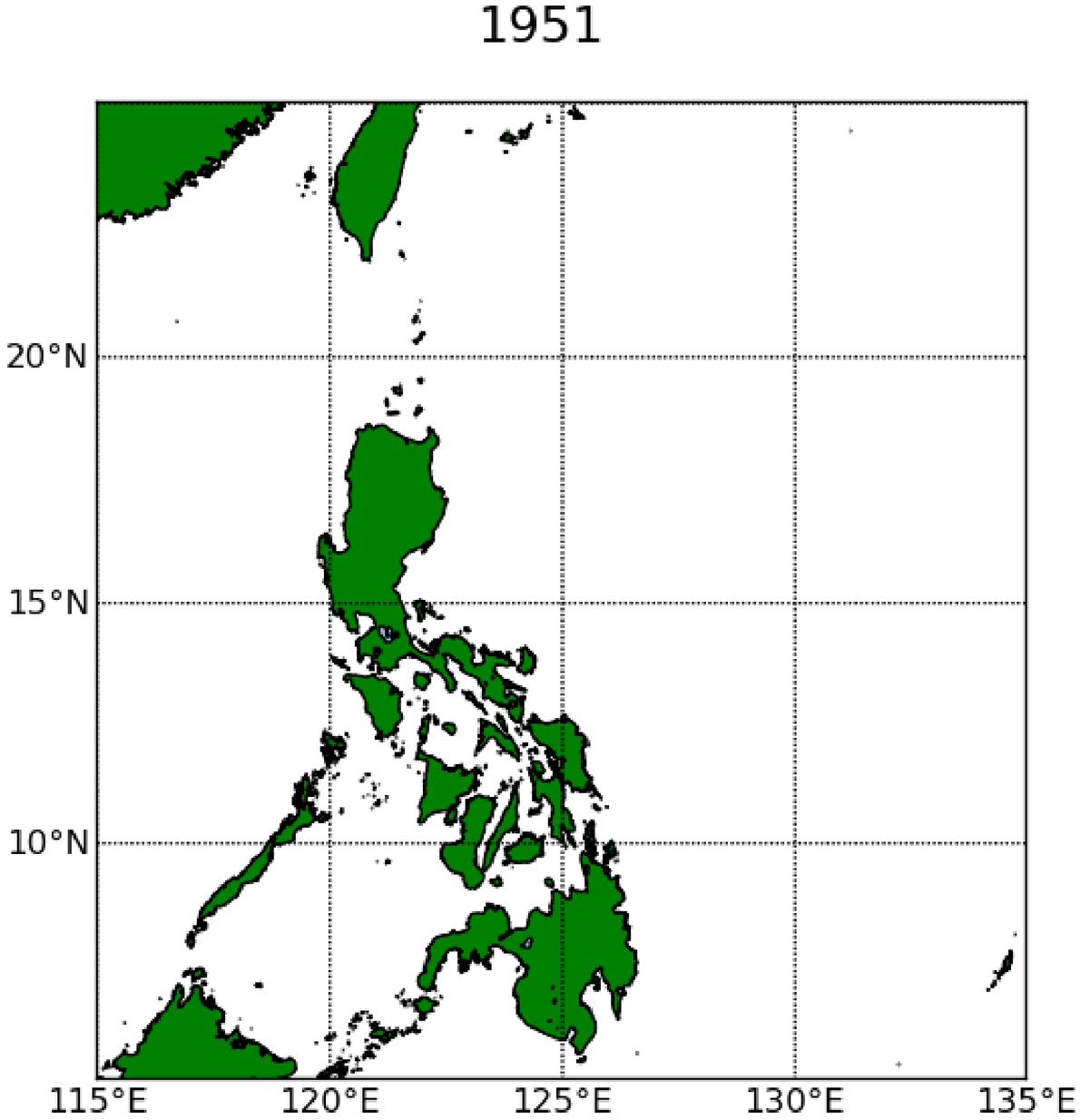
The Data Privacy Act of 2012

Privacy Resilience

with Local Government Units

NATIONAL PRIVACY COMMISSION

DP LOCAL GOVERNMENT UNITS 11


1951
20°N
15°N
10°N
115°E
120°E
125°E
130°E
135°E

RESILIENCE AND THE FILIPINO SPIRIT

RESILIENCE AND THE FILIPINO SPIRIT

RESILIENCE AND THE FILIPINO SPIRIT

Resilience

- **Resilience**
- **rɪˈzɪlɪəns/**
- ***noun***
- **1.the capacity to recover quickly from difficulties; toughness.**
  - **adapt well to change**
  - **keep going in the face of adversity**

CYBER ATTACKS (REAL-TIME) *2017*

Norse – Superior Attack Intelligence

Norse maintains the world's largest dedicated threat intelligence network. With over eight million sensors that emulate over six thousand applications – from Apple laptops, to ATM machines, to critical infrastructure systems, to closed-circuit TV cameras - the Norse Intelligence Network gathers data on who the attackers are and what they're after. Norse delivers that data through the Norse Appliance, which pre-emptively blocks attacks and improves your overall security ROI, and the Norse Intelligence Service, which provides professional continuous threat monitoring for large networks.

LIVE ATTACKS

Timestamp	Attacker	Attacker IP	Attacker Geo	Target Geo	Attack Type	Port
14:56:21.719	Microsoft Corporation	207.46.100.252	Redmond, US	De Kalb Junction, US	smtp	25
14:56:21.284	This Ip Network Is Used For Internet Security Research. Int	185.35.62.250	Geneve, CH	Dubai, AE	ntp	123
14:56:20.770	Philippine Long Distance Telephone Company	122.3.47.120	Paranaque, PH	Lynnwood, US	telnet	23
14:56:20.580	Microsoft Corporation	65.55.169.249	Washington, US	De Kalb Junction, US	smtp	25
15:05:41.557	Philippine Long Distance Telephone Company	122.54.132.220	Makati, PH	Dubai, AE	telnet	23
:19.784	Microsoft Corporation	207.46.100.250	Redmond, US	De Kalb Junction, US	smtp	25
15:04:02.333	Philippine Long Distance Telephone Company	122.3.47.120	Paranaque, PH	Lynnwood, US	telnet	23

Privacy Risk Formula

Privacy Risk = Probability of a Problematic Data Action * Impact of a Problematic Data Action

Probability is a contextual analysis that a data action is likely to create a problem for a representative set of individuals

Impact is an analysis of the costs should the problem occur

What is a Privacy Risk?

A Personal Data Breach or a Data Privacy Violation that has NOT happened yet.

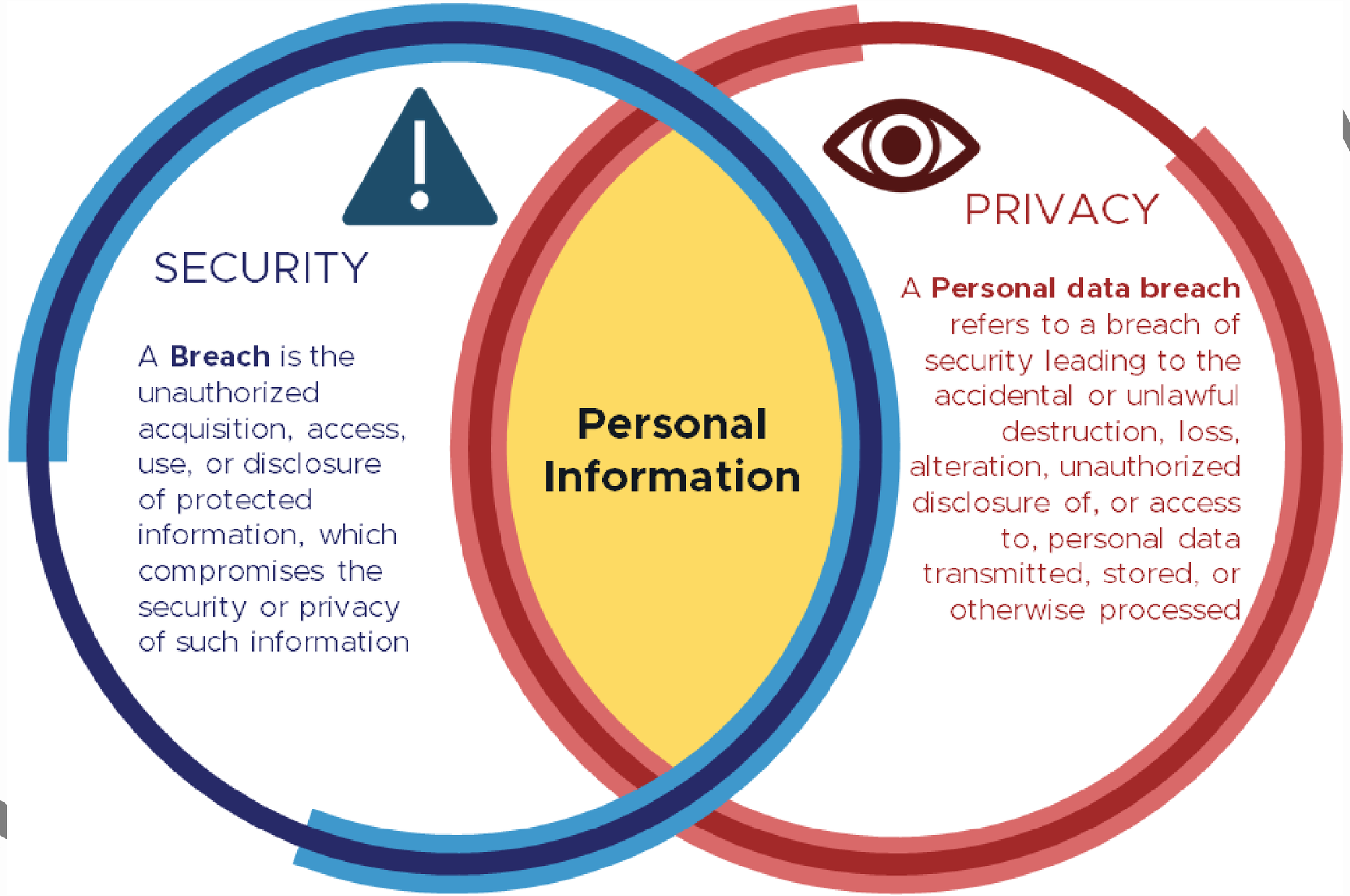
What is Privacy Resilience?

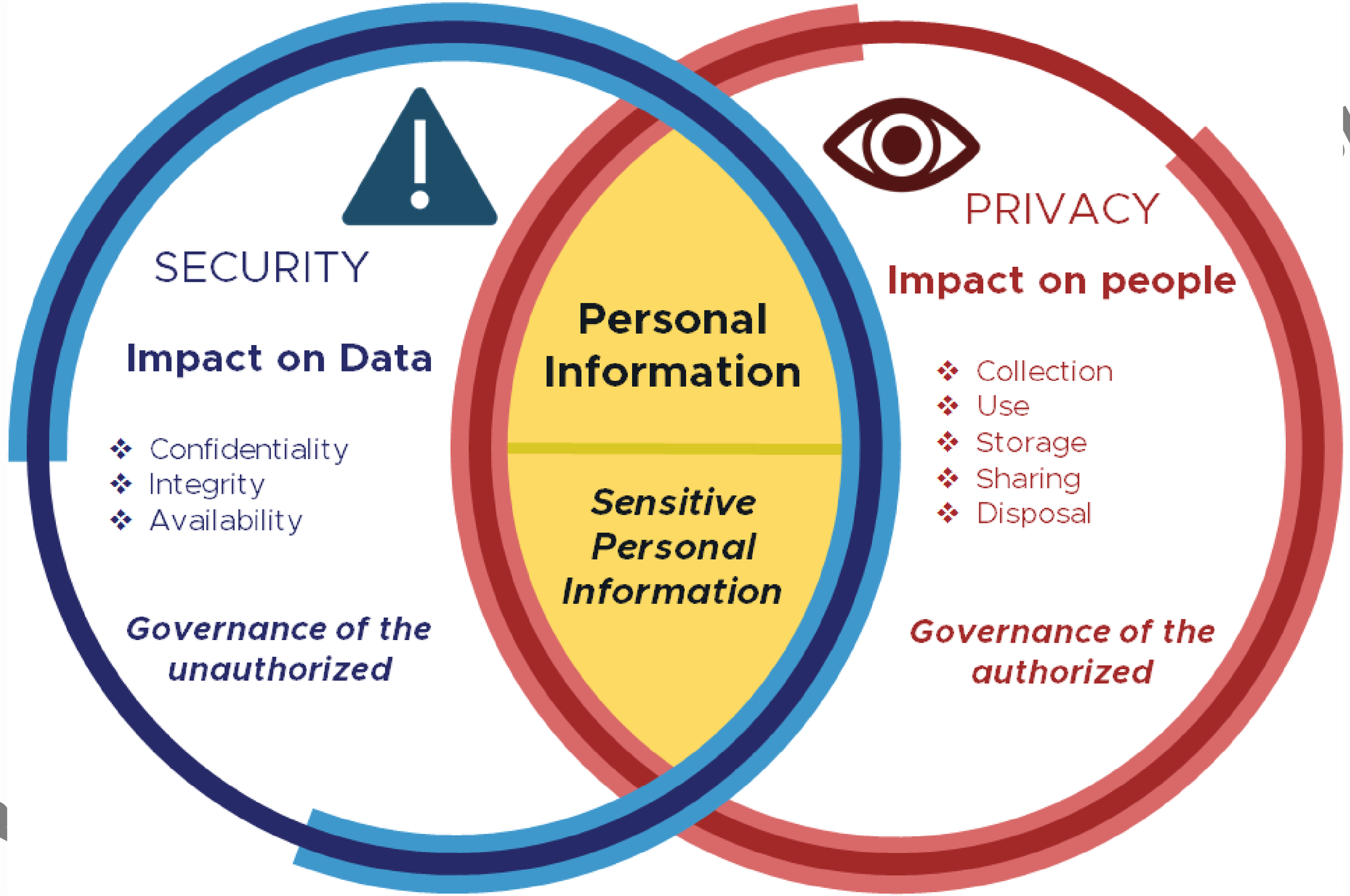
A Personal Data Breach or a Data Privacy Violation that was prevented.

A breach and privacy disaster that did not happen.

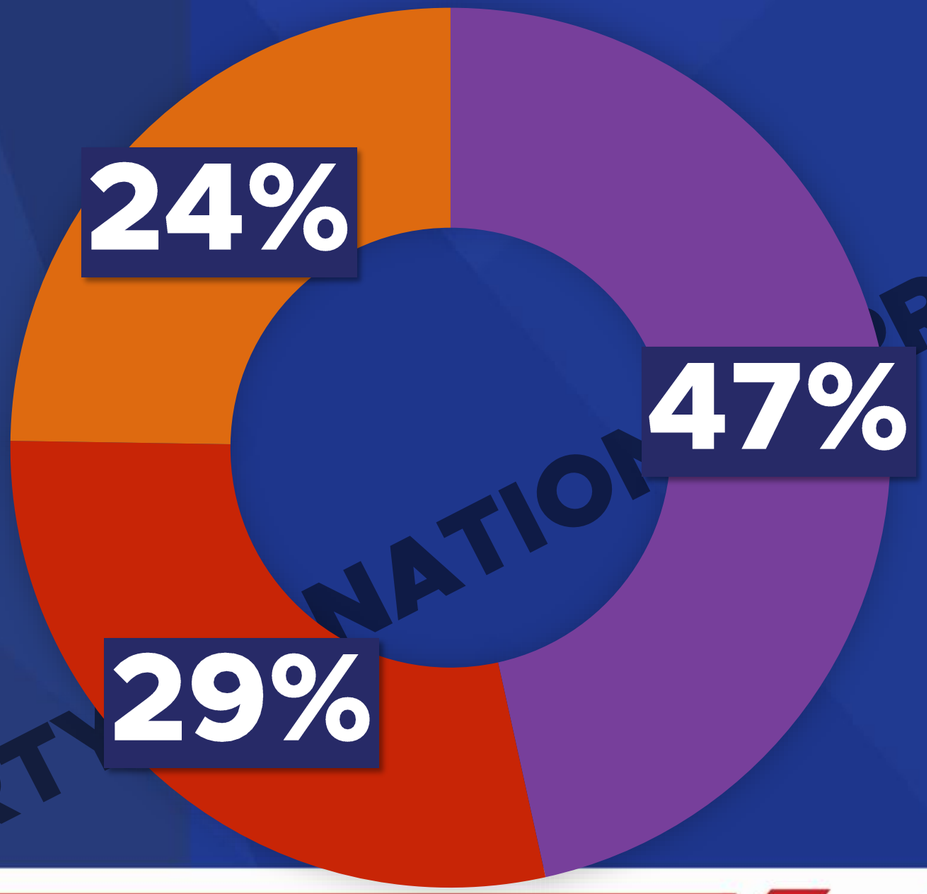
Disaster

Resilience


SECURITY
A **Breach** is the unauthorized acquisition, access, use, or disclosure of protected information, which compromises the security or privacy of such information
Personal Information
PRIVACY
A **Personal data breach** refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed


SECURITY
Impact on Data
Confidentiality
Integrity
Availability
Governance of the unauthorized
Personal Information
Sensitive Personal Information
PRIVACY
Impact on people
Collection
Use
Storage
Sharing
Disposal
Governance of the authorized

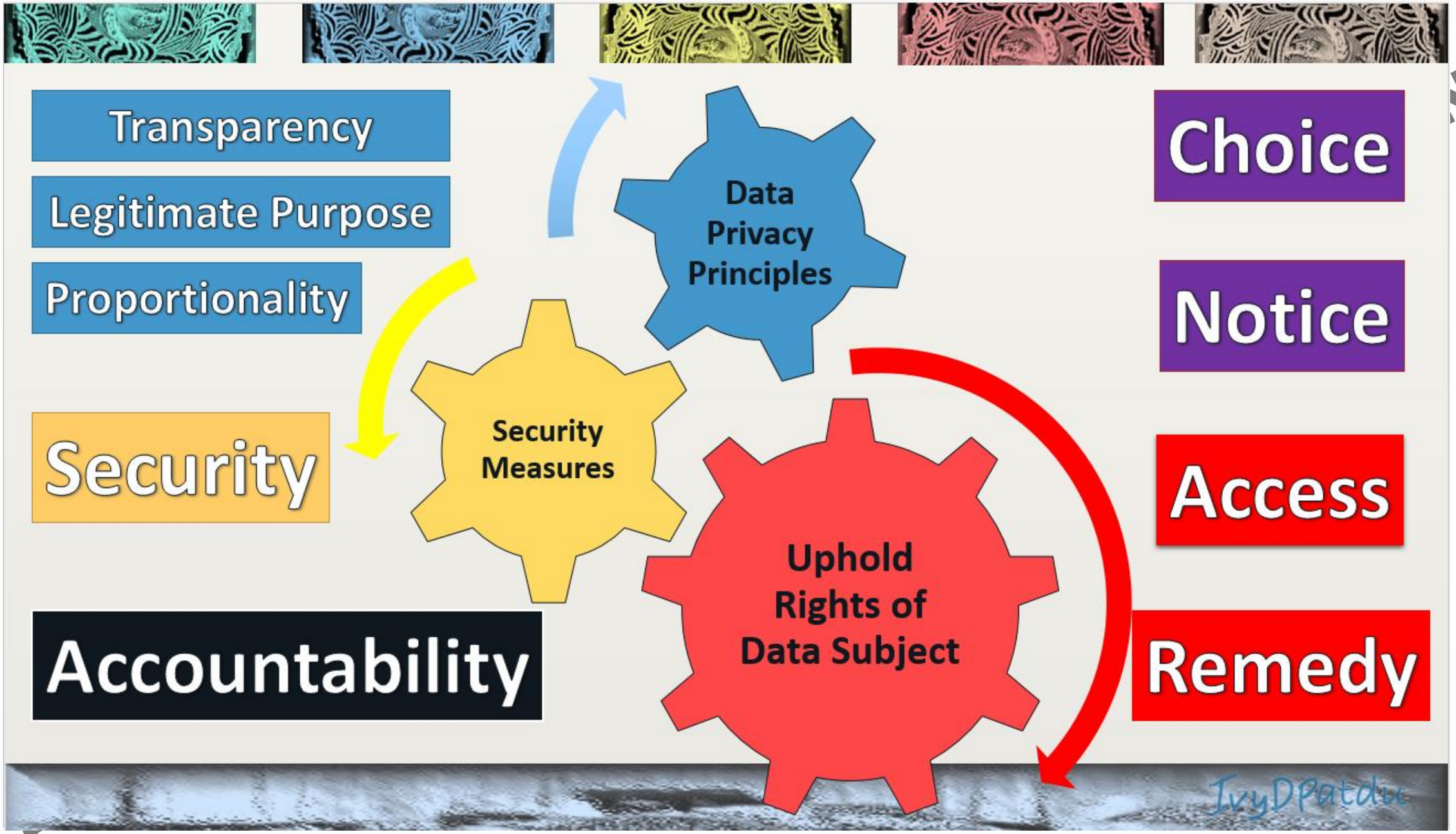
ROOT CAUSES OF BREACH



- Malicious or criminal attack
- System Glitch
- Human Error

Ponemon Institute LLC, *2015 Cost of Data Breach Study: Global Analysis*, May 2015, p. 10


A. 10
NATIONAL
PRIVACY
COMMISSION


Transparency
Legitimate Purpose
Proportionality
Data Privacy Principles
Choice
Notice
Security
Security Measures
Access
Uphold Rights of Data Subject
Accountability
Remedy
IvyDPatdu

The NPC's 5 Pillars of Accountability

1

Commit to Comply:
APPOINT A DATA PROTECTION OFFICER

2

Know Your Risks:
CONDUCT A PRIVACY RISK OR IMPACT ASSESSMENT

3

Write Your Plan:
CREATE A PRIVACY MANAGEMENT PROGRAM

4

Be Accountable:
IMPLEMENT YOUR PRIVACY AND DATA PROTECTION MEASURES

5

Be Prepared for Breach:
REGULARLY EXERCISE YOUR BREACH REPORTING PROCEDURE

NATIONAL PRIVACY COMMISSION

DP LOCAL GOVERNMENT UNITS 11

DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK

I. GOVERNANCE

A. Choose a DPO

II. RISK ASSESSMENT

B. Register
C. Records of processing activities
D. Conduct PIA

III. ORGANIZATION

E. Privacy Management Program
F. Privacy Manual

IV. DAY TO DAY

G. Privacy Notice
H-O. Data Subject Rights
P. Data Life Cycle

V. DATA SECURITY

Q. Organizational
R. Physical
S. Technical
- Data Center
- Encryption
- Access Control Policy

VI. BREACHES

T. Data Breach Management;
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Document
- Breach Notification

VII. THIRD PARTIES

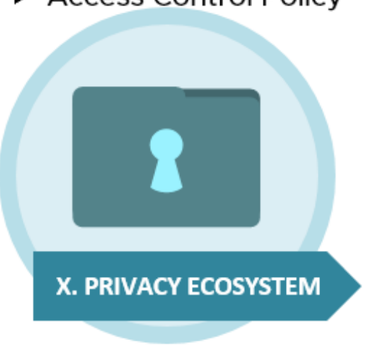
U. Third Parties;
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

VIII. MANAGE HR

V. Trainings and Certifications
W. Security Clearance

IX. CONTINUITY

X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations



X. PRIVACY ECOSYSTEM

Y. New technologies and standards
Z. New legal requirements

NATIONAL PRIVACY COMMISSION

DEVELOPING A PRIVACY MANAGEMENT PROGRAM

Government

NATIONAL PRIVACY COMMISSION

DP LOCAL GOVERNMENT UNITS 11

Why create a **Privacy Management** Program?

- **Easier to Explain to Staff and Management: results & benefits**
- **Compliance becomes more manageable: outline of how**
- **Save on avoidable 'clean-up' expenses: stronger safeguards**

NATIONAL PRIVACY COMMISSION

DPO LOCAL GOVERNMENT UNITS 11

Key Components of a **Privacy Management** Program

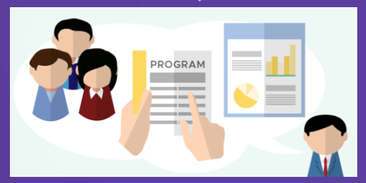
Organizational Commitment

Governance Structure

Program Controls

Ensure Implementation

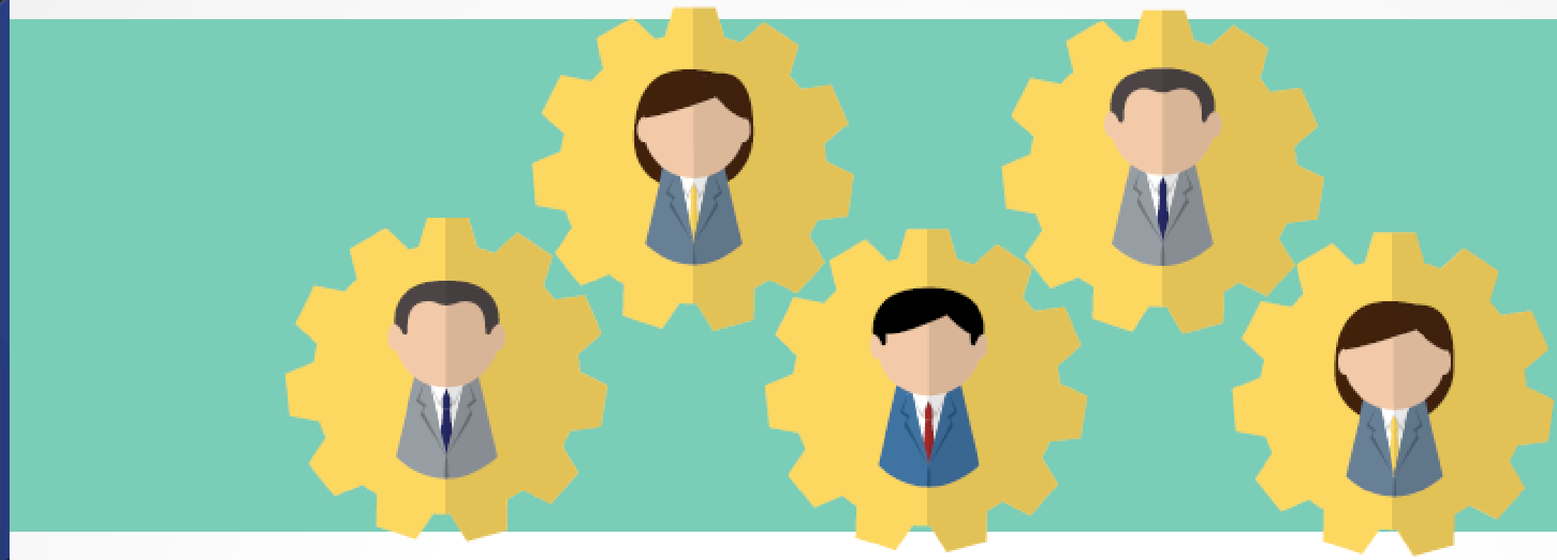
Continue Development



Review and Revise Programs

Key Components of a **Privacy Management** Program

Organizational Commitment



Organizations (both public and private) should develop and implement a PMP that give effect to the data privacy principles of the Data Privacy Act of 2012 (RA 10173), specifically Sec 11, Chapter III. This means creating a governance structure, or at the minimum, processes to follow and the mechanism to ensure that they are being followed.

Organizational Commitment

1.1 BUY-IN FROM THE TOP

Top management support is key to a successful PMP and essential for the emergence of a culture of privacy in the organization.

When top management is committed to ensuring that the organization is accountable, the program will have a better chance of success, and a **privacy respectful culture** will more likely be established.

This means that top management should:

Appoint the Data Protection Officer(s);

Endorse a set of program controls; and

Report to the Board, as appropriate, on the program.

Organizational Commitment

1.2 THE DATA PROTECTION OFFICER

A Data Protection Officer should be appointed or designated to manage the privacy management program. The Data Protection Officer shall be responsible for **structuring, designing and managing the privacy management program,** including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up.

Specifically, the Data Protection Officer shall:

establish and implement program controls;

continuously assess and revise program;

coordinate with those who are responsible for related disciplines and functions within the organization;

represent the organization in the event of an inspection or an investigation by the National Privacy Commission; and

advocate personal data protection within the organization itself.

Organizational Commitment

1.3 REPORTING

The organization/agency should establish **internal reporting mechanisms** to ensure that the privacy management program is structured and whether it is functioning as expected. In larger organizations, the audience for this information is likely to be top management, and in turn, top management reports to the board of directors. All reporting mechanisms should be reflected in the organization's/agency's program controls.

An effective reporting program has the following characteristics:

clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach;

tests and reports on the results of its internal reporting

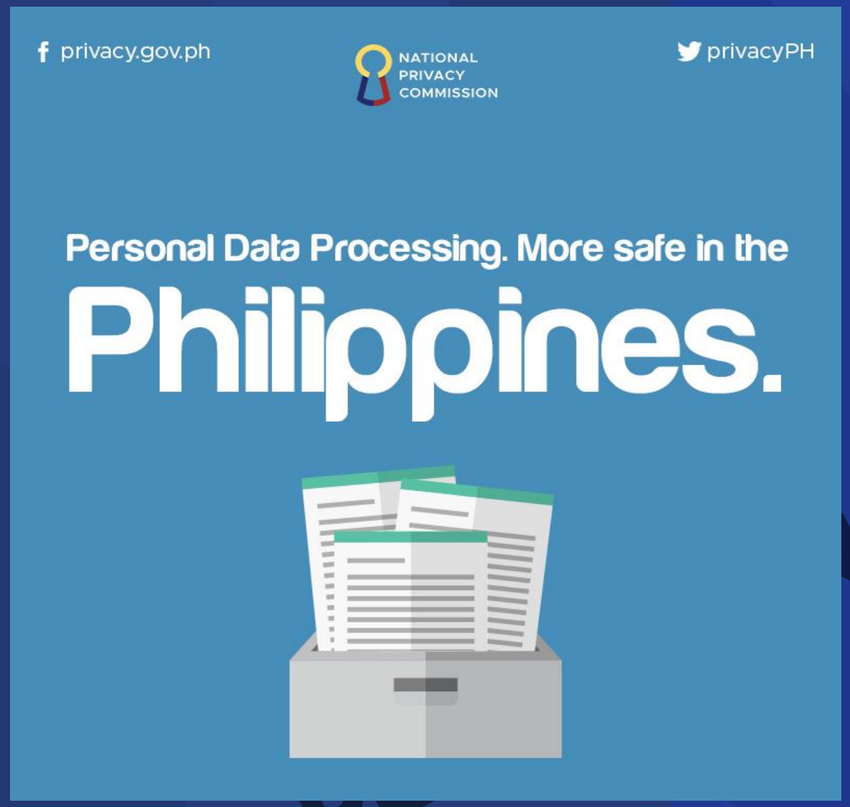
documents all of it
reporting structure

Key Components of a **Privacy Management** Program

Program Controls

These help ensure that what is mandated in the governance structure is implemented in the organization/agency. Developing these controls will assist the Data Protection Officer in structuring an appropriate privacy management program within the organization/agency. Controls also demonstrate how the organization/agency is compliant with the Data Privacy Act.

Program Controls



2.1 PERSONAL DATA INVENTORY

An organization/agency should know **what kinds** of personal data it holds, **how** the personal data is being used, and whether the organization/agency really **needs** it at all.

Understanding and documenting the types of personal data that an organization collects and where it is held (e.g. whether or notwhether the data has been passed to any data controller) are important. This will affect **the type of consent** the organization/agency obtains from individuals and how the data is protected; and it will make it easier to assist individuals in exercising their data access and correction rights. Every component of an accountable, effective PMP begins with personal data inventory.

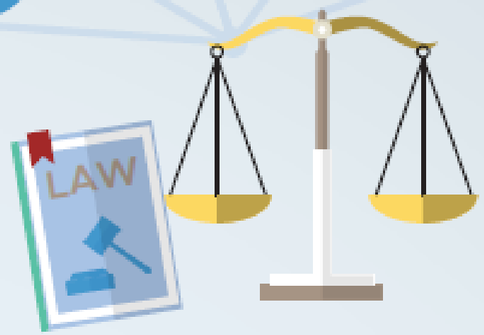
Every organization/agency should document:

- the kinds of personal data it holds and where it is held (i.e. within the organization or by the data controller(s)); and
- the reason(s) why it is collecting, using or disclosing personal data.

Program Controls

2.2 POLICIES

Organizations/agencies should develop and document internal policies that **address obligations** under the law. These policies should be made available to all employees and updated periodically.



Organizations/agencies should develop internal policies that give effect to the **data protection principles** in the law. These policies should be documented and should show how they connect to the legal requirements.

Program Controls

Collection of personal data;

Accuracy and retention of personal data;

Use of personal data including the requirements for consent;

Security of personal data;

Transparency of organizations/agencies' personal data policies and practices; and

Access to and correction of personal data.

Program Controls

2.3 RISK ASSESSMENT TOOLS

Proper use of risk assessment tools can help prevent problems. Fixing a personal data problem after the fact can be costly. Therefore it is vital that **careful consideration of the purposes** for a particular initiative, product or service, and an assessment that minimizes any personal data impacts is done.

Program Controls

2.4 CAPACITY BUILDING

In order for the PMP to be effective, relevant employees should be **made aware** of personal data protection generally and to be conversant with the organizations/agencies' policies and practices for compliance with the law. Those who handle personal data directly may **need additional training** specifically tailored to their roles. Training and education need to be current.

Program Controls

For personal data protection training and education to be effective, it should:

Be given to new employees and periodically thereafter;

Cover the policies and procedures established by the organization;

Be delivered in an appropriate and effective manner, based on organizational needs; and

Circulate essential information to relevant employees as soon as practical if an urgent need arises.

Program Controls

2.5 BREACH HANDLING

Personal data breaches are expensive and could lead to loss of trust.

Organizations/agencies should have a **procedure** in place and an officer or **a designated team** responsible for managing a personal data breach. Responsibilities for internal and external reporting of the breach should be clear.

In handling personal data breach, organizations/agencies should **consider the circumstances** of the breach, and decide whether any of the following persons should be notified as soon as practicable:

The affected data subjects

The law enforcement agencies;

The National Privacy Commission;

Any relevant regulators;

Program Controls

2.7 COMMUNICATION

Organizations/agencies should take all **practical steps** to ensure employees and customers/citizens can ascertain their personal data policies and practices.

Communication should be **clear and easily understandable** and not simply a reiteration of the Data Privacy Act. In general, it should:

Provide enough information so that the public knows the purpose of the collection, use and disclosure of personal data and how long it is retained;

Include information on who to contact with questions or concerns;

Be made easily available to individuals.

Key Components of a **Privacy Management** Program

Continue Development

CONTINUING ASSESSMENT AND DEVELOPMENT

In order to properly protect personal data and meet legal obligations, organizations/agencies should monitor, assess and revise their privacy management framework to ensure it remains relevant and effective.

NATIONAL PRIVACY COMMISSION

DP LOCAL GOVERNMENT UNITS 11

Continue Development

I. DEVELOP AN OVERSIGHT AND REVIEW PLAN

An oversight and review plan will help the organization keep its PMP on track and up-to-date.

The Data Protection Officer should develop an oversight and review plan on a periodic basis that sets out how and when the PMP's effectiveness will be **monitored and assessed.** Depending on the organization/agency's compliance and control infrastructure, such plan may be covered in its overall oversight and review system.

The oversight and review plan should establish performance measures and include a schedule of when the policies and other program controls will be reviewed.

Continue Development

II. ASSESS AND REVISE PROGRAM CONTROLS

The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised.

Continue Development

Monitoring, an ongoing process, should address the following questions:

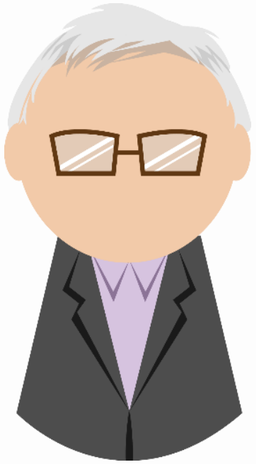
What are the latest threats and risks?

Are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the National Privacy Commission?

Are new services being offered that involve increased collection, use or disclosure of personal data?

Is training necessary? If yes, is it taking place? Is it effective? Are policies and procedures being followed? And, Is the training program up to date?

PRIVACY.GOV.PH



facebook.com/privacy.gov.ph
twitter.com/privacyph
info@privacy.gov.ph

Way forward: Compliance of LGUs to the DPA

- *Appointment of a DPOs / COPs*
  - *Capacity Building*
    - *DPO Workshop Liga ng mga Barangay – Davao City Chapter*
- *Know your risks (Privacy Impact Assessment)*
  - *Inventory of data and assess data process flows*
- *Develop your Privacy management plan based on the risks assessed*
  - *Issuance of Ordinances related to the DPA*
- *Implement and communicate your Data Privacy Plan*
- *Prepare for a breach*

NATIONAL PRIVACY COMMISSION

DP 11
LOCAL GOVERNMENT UNITS